5.3 ネットワークのトラブルシューティング

Webページの閲覧だけができない、あるいはメールの送受信だけができないというような、部分的なトラブルは、原因の特定や対処がしやすいトラブルといえます。しかし、すべてのアプリケーションが利用できない、あるいはサービスが利用できないという症状の場合は、原因としてはさまざまな要素が考えられるため、原因を特定しづらくなります。

ネットワークのトラブルシューティング手法は、近いところから遠いところへ、ネットワークの下位層から上位層へと解析を進めていきます。

最初に、pingの疎通確認で、範囲を確定します。

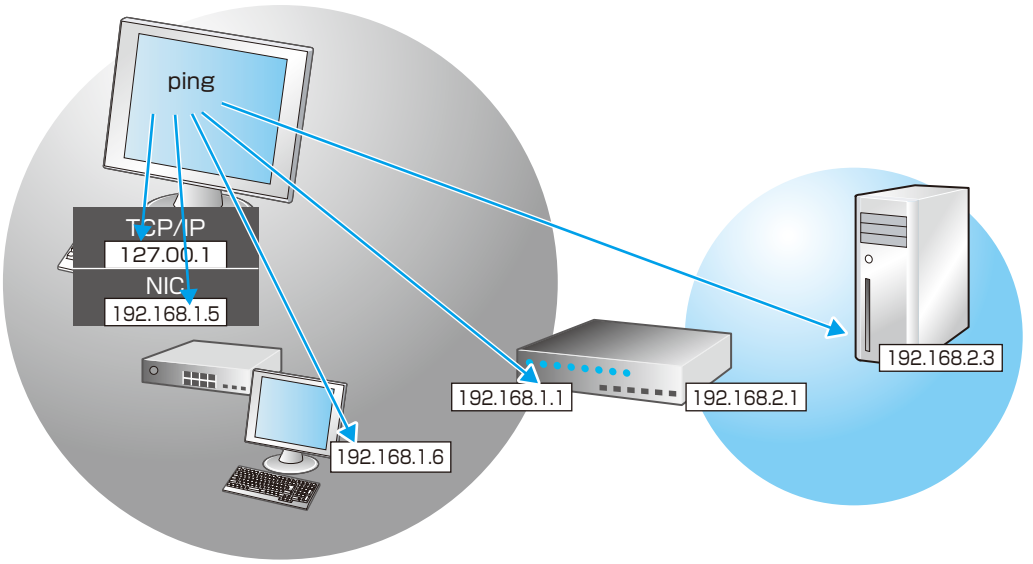


図5.11　pingによる疎通確認

pingには確認する順番があるので以下に示します。

① ping 127.0.0.1（ループバックアドレス）
② ping 自身のIPアドレス
③ ping 同じネットワーク上のホスト
④ ping デフォルトゲートウェイ
⑤ ping リモートホスト

① TCP/IPがインストールされていて正常に動作している場合は、ループバックアドレスでリプライが返ってきます。リプライが返ってこない場合、なんらかの原因でサービスが無効になっていたり、TCP/IPプロトコルが壊れていたりする可能性があります。

② 自身のIPアドレスは、TCP/IPのプロパティの画面から確認するのではなく、ipconfigコマンドで、正しいIPアドレスを確認します。自身のIPアドレスでpingの返答がない場合、NICが壊れている可能性があります。デバイスマネージャなどで、NICの状態を確認します。

③ 同じネットワーク上のホストにpingして返答がない場合、ケーブル、スイッチを疑います。スイッチのポートのリンクランプを確認し、ポートが動作しているか確認します。

周囲のコンピュータがすべて接続できないという場合、それが狭い範囲であれば、スイッチが原因と思われます。

スイッチの電源が入っているかどうかを確認し、次に各ポートのリンクランプを確認します。各ポートのリンクランプは、電源がオンになっているパソコンやネットワーク機器が正しく接続されている場合には点灯もしくは点滅しています。

④ デフォルトゲートウェイにpingして返答がない場合、ルータがダウンしているか、ルータのIPアドレスを間違えていないかを確認します。

⑤ リモートホストの返答がない場合、ルーティングできているか、リモートホストがダウンしていないかを確認します。

5.3.1 各種サーバ

サーバは多数のクライアントにサービスを提供するため、サーバのトラブルは広範囲に影響します。

コンピュータが通信できない場合、IPアドレスが取得されているか、また名前解決ができているかを確認します。IPアドレスが取得されていない場合は、DHCP（Dynamic Host Configuration Protocol）サーバを確認する必要がありますし、名前解決ができないという場合は、DNS（Domain Name System）サーバを確認する必要があります。

NOTE

リンクランプ：スイッチやNICにあるランプで、相手と正常に接続できていれば点灯します。

5.3.2　DHCP（Dynamic Host Configuration Protocol）

DHCPは、クライアントにIPアドレスの貸し出しをするサーバです。DHCPサーバからアドレスが借りられないと、DHCPクライアントは、通信することができません。

■ ipconfigによるDHCPクライアント側でのトラブルシューティング

最初は、IPアドレスが取得できているか確認をします。

以下のコマンドを使用します。

ipconfig /all

ここで確認するのは、アドレスが借りられていること、DHCPサーバのアドレス、有効期間です。

アドレスが借りられず、再要求をかけるには、ipconfig /renewを使用します。

アドレスを返却するには、ipconfig /release を使用します。

■ DHCPサーバ側でのトラブルシューティング

DHCPサーバとDHCPクライアントの間には、いくつかのメッセージのやり取りがあります。このメッセージの内容を知ることで、現在どのような状況にあるのか、判断することが出来ます。

このメッセージは、サーバ上の統計情報で確認することができます。どのようなメッセージが存在するかにより、トラブルの原因がつかめる場合があります。

DHCP管理コンソールのサーバのアイコンを右クリックし「統計情報の表示」をクリックします。

画面5.12　DHCPの統計情報

表5.9に統計情報の内容を示します。

表5.9　統計情報の内容

統計情報	関連メッセージ	説明
開始時間	―	DHCPサービスが開始された時刻
稼働時間	―	DCHPがアクティブである時間
発見	DHCP DISCOVER	クライアントがサーバを発見するためのメッセージ
提供	DHCP OFFER	サーバからクライアントへの設定値候補を通知するメッセージ
要求	DHCP REQUEST	クライアントが決定したサーバへの取得依頼メッセージ
ACK	DHCP ACK	サーバからクライアントへの取得正常終了メッセージ
NACK	DHCP NAK	サーバからクライアントへの取得拒否メッセージ
拒否	DHCP DECLINE	クライアントからサーバへの拒否メッセージ
解放	DHCP RELEASE	クライアントからサーバへのリリース要求メッセージ
使用中	―	現在リースされているIPアドレスの数
利用可能	―	リース可能なIPアドレスの数

クライアントにIPアドレスがリースできないのは、貸し出すIPアドレスがなくなってしまった場合や、サービスがダウンしている場合などが考えられます。

画面5.13　DHCPサーバの管理画面

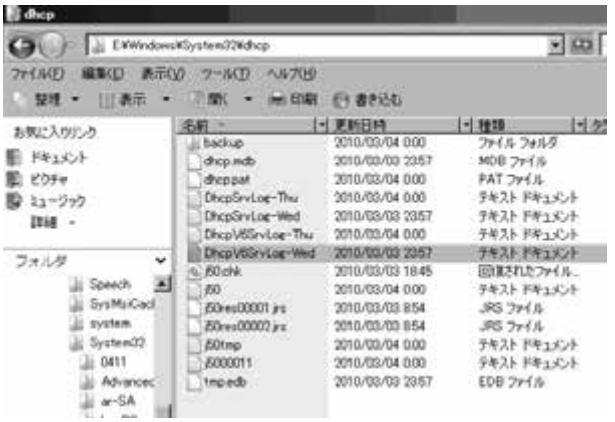
DHCPサーバの管理コンソールを開き、サーバアイコンの状態を確認します。(画面5.13)

通常、緑の上向き矢印は正常に動作していることを表しますが、赤の下向き矢印は機能していないことを表し、エクスクラメーションマーク(!)はアドレスが不足していることを示しています。

DHCPサーバのログにより、どのクライアントにどのIPアドレスをリースしたか、またサービスがスタートした時間などの情報が得られます。

DHCPサーバのログは、Windows¥System32¥dhcp フォルダ内に毎日0時になると曜日ご

とのログファイルが生成されます。



画面5.14　DHCPサーバのログファイル

■ 未承認DHCP

Active Directory内のWindows NT以降のDHCPサーバは認証されて動作します。これは、いたずらにDHCPサーバを立て、クライアントに間違ったIPアドレスをリースしないようにするためです。例えば、既にDHCPサーバが動いているワークグループと同じネットワーク上にドメインを構築した場合、既存のDHCPサーバはドメインに所属するクライアントに対しては機能しません。その際は、ドメインの管理権限を使用し、承認を得てドメインにDCHPサーバを追加します。

画面5.15　DHCPサーバの承認

5.3.3　DNS（Domain Name System）

DNSサーバは名前解決を提供するサーバです。DNSがダウンしていると名前解決ができず、通信ができません。

■ nslookupによるDNSクライアント側でのトラブルシューティング

nslookup は、ホスト名をIPアドレスに解決する、レコードの問い合わせを行うコマンドです。

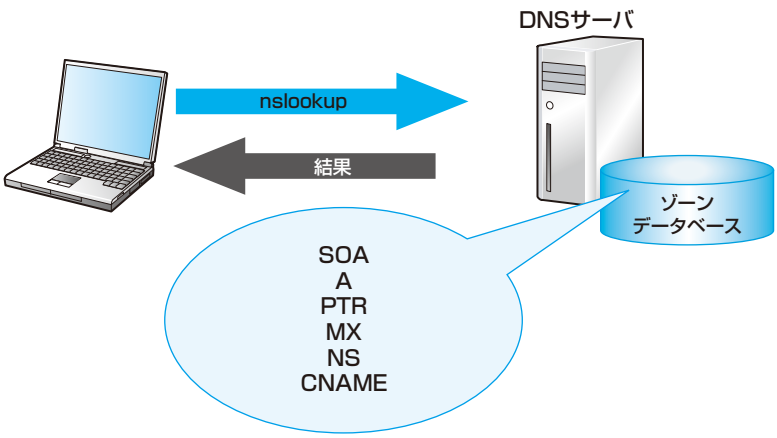


図5.12　nslookupコマンドによる問合せ

コマンドは、対話モードと非対話モードがあります。nslookupをそのまま実行すると、対話モードになり、プロンプトが表示されて、問合せを行なう入力待ち状態となります。終了するときは、exitと入力します。（画面5.16）

```
C:¥>nslookup
Default Server:  dns01.pc-seibishi.local
Address:  10.1.0.11

> www.pc-seibishi.org
Server:  dns01.pc-seibishi.local
Address:  10.1.0.11

Name:    sv.pc-seibishi.org
Address:  202.221.143.228
Aliases:  www.pc-seibishi.org

> exit
C:¥>
```

画面5.16　nslookup 対話モード

非対話モードの場合は、nslookup ホスト名 と指定します。(画面5.17)

```
C:¥>nslookup www.pc-seibishi.org
Server:  dns01.pc-seibishi.local
Address:  10.1.0.11

Name:    sv.pc-seibishi.org
Address:  202.221.143.228
Aliases:  www.pc-seibishi.org

C:¥>
```

画面5.17　nslookup 非対話モード

■ ipconfigによるDNSクライアント側でのトラブルシューティング

ipconfigを使用して、クライアント側のトラブルシュートを行うことができます。

・ipconfig /displaydns

DNSクライアントは名前解決キャッシュ（リゾルバキャッシュ）を持ち、通信の度にDNSに問い合わせないようにしています。ipconfig /displaydnsコマンドを使うと、hostsファイルから事前読み込みされた情報と、DNSによって最近取得された情報の両方が表示されます（画面5.18）。

```
C:¥>ipconfig /displaydns

Windows IP Configuration

    www.pc-seibishi.org
    ----------------------------------------
    Record Name . . . . . : www.pc-seibishi.org
    Record Type . . . . . : 5
    Time To Live  . . . . : 83225
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    CNAME Record  . . . . : sv.pc-seibishi.org

C:¥>
```

画面5.18　ipconfig / displaydns 実行結果

・ipconfig /flushdns

例えばWebサーバの入れ替えなどで、問い合わせたいWebサーバのIPアドレスが変わった場合、クライアントのリゾルバキャッシュは更新されませんので、Webサーバにアクセスできなくなります。その際は、ipconfig /flushdnsコマンドを使って、クライアントのリゾルバキャッシュの内容を消去する必要があります（画面5.19）。

なお、リゾルバキャッシュの削除を行ったのにもかかわらず、キャッシュが表示されている場合は、クライアントのhostsファイルに書き込まれている可能性があります。

NOTE

hostsファイル:ホスト名とIPアドレスとを静的に変換するファイルのことで、システムファイルとして存在しています。DNSによるドレス変換よりも優先されます。

```
C:¥>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:¥>
```

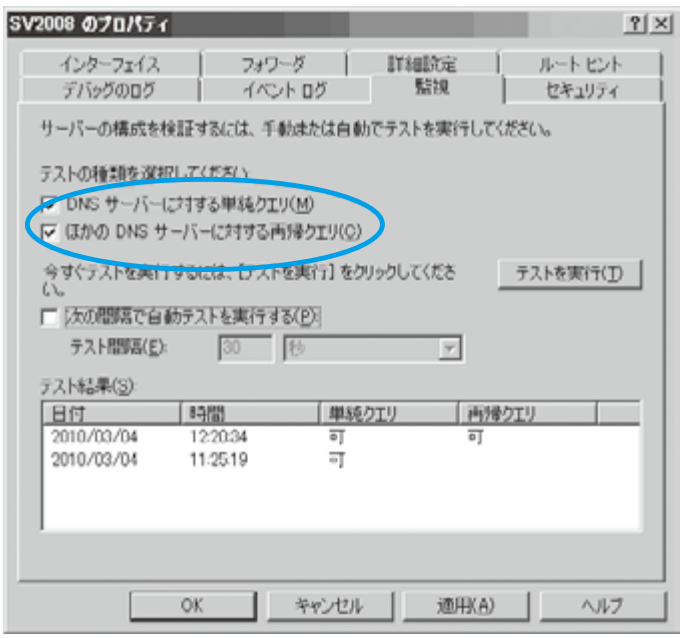
画面5.19　ipconfig /flushdns 実行結果

■ DNSサーバ側のトラブルシューティング

DNSサーバは、ログや監視ツールが複数ありますので、以下に代表的なものを説明します。

・DNSクエリ

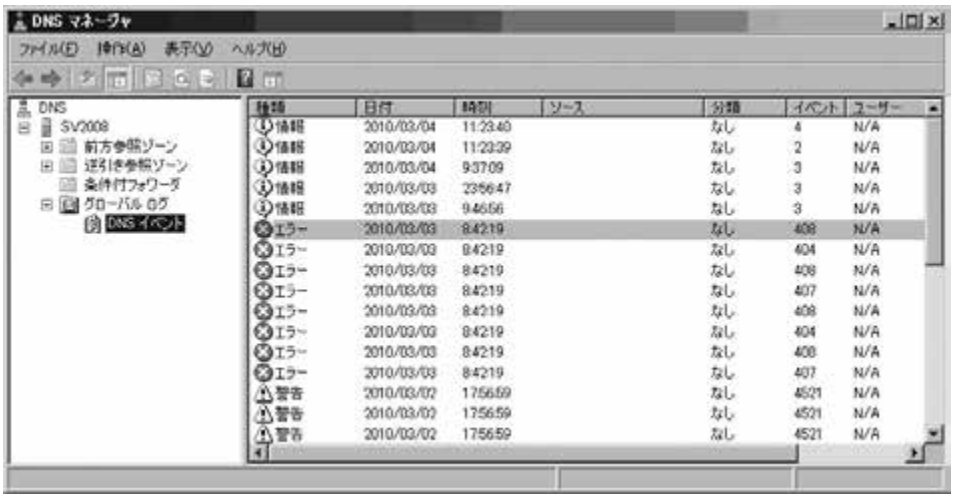
「DNSサーバに対する単純クエリ」と「ほかのDNSサーバに対する再帰クエリ」を確認することができます。画面5.20の〔テストを実行〕ボタンから実行します。



画面5.20　DNSクエリの確認設定

・DNSイベントログとデバッグログ

DNSイベントログでは、「ゾーン転送情報の監視」、「コンピュータのイベントの監視」を行います。



画面5.21　DNSイベントログ

DNSイベントログは、サーバのプロパティより、イベントのログをどのように取得するか設定します（画面5.22）

画面5.22　DNSイベントログの設定

デバッグログでは、DNSの動作に関する詳細な情報を表示します。ログは膨大なため、一時的な利用にとどめます。通常、Windows¥system32¥dns¥dns.logに保存されますが、ログファイルのパスを入力し使用することもできます（画面5.23）。

画面5.23　ログファイルの設定

DNSのエラーは、Active Directoryのドメイン環境では、ドメインの管理者がトラブルシュートを行う場合がほとんどです。Active Directoryを保持するドメインコントローラにDNSがインストールされている場合は、ドメインの管理者権限でトラブルシュートを行います。